Terms used: **compression encryption generating encryption key from compressed data**

Found **1,025** of **206,720**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Applied cryptography: Attacking and repairing the winZip encryption scheme

Tadayoshi Kohno

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available: pdf(171.91 KB) Additional Information: full citation, abstract, references, index terms, review

WinZip is a popular compression utility for Microsoft Windows computers, the latest version of which is advertised as having "easy-to-use AES encryption to protect your sensitive data." We exhibit several attacks against WinZip's new encryption method, dubbed "AE-2" or "Advanced Encryption, version two." We then discuss secure alternatives. Since at a high level the underlying WinZip encryption method appears secure (the core is exactly Encrypt-then-Authenticate using AES-CTR and HMAC-SHA1), ...

Keywords: WinZip, Zip, applied cryptography, attacks, compression, encryption, security fixes

2 Storing text retrieval systems on CD-ROM: compression and encryption considerations

Shmuel T. Klein, Abraham Bookstein, Scott Deerwester

July 1989 **ACM Transactions on Information Systems (TOIS)**, Volume 7 Issue 3

Publisher: ACM Press

Full text available: pdf(1.53 MB) Additional Information: full citation, abstract, references, citings, index terms, review

The emergence of the CD-ROM as a storage medium for full-text databases raises the question of the maximum size database that can be contained by this medium. As an example, the problem of storing the Trésor de la Langue Fran&ccidel;aise on a CD-ROM is examined in this paper. The text alone of this database is 700 megabytes long, more than a CD-ROM can hold. In addition, the dictionary and concordance needed to access these data must be stored. A further constraint is that some of th ...

3 A fast MPEG video encryption algorithm

Changgui Shi, Bharat Bhargava

September 1998 **Proceedings of the sixth ACM international conference on Multimedia MULTIMEDIA '98**
Publisher: ACM Press
Full text available: pdf(805.58 KB) Additional Information: full citation, references, citings, index terms

Keywords: DES, MPEG codec, MPEG video encryption, multimedia data security

4 Methods for encrypting and decrypting MPEG video data efficiently

Lei Tang
February 1997 **Proceedings of the fourth ACM international conference on Multimedia MULTIMEDIA '96**
Publisher: ACM Press
Full text available: pdf(1.45 MB) Additional Information: full citation, references, citings, index terms

Keywords: MPEG codec, compression, multimedia commerce, multimedia encryption, multimedia security

5 Content analysis: A novel encryption algorithm for high resolution video

Fuwen Liu, Hartmut Koenig
June 2005 **Proceedings of the international workshop on Network and operating systems support for digital audio and video NOSSDAV '05**
Publisher: ACM Press
Full text available: pdf(335.72 KB) Additional Information: full citation, abstract, references, index terms

The popularity of multimedia applications is rapidly growing nowadays. The confidentiality of video communication is of primary concern for their commercial use, e.g. in video on demand services or in multiparty video conferences. Specific video encryption algorithms are strongly required in real-time multimedia communication to fulfill the strict timing requi-rements. In this paper we present a novel video encryption algorithm, called *Puzzle*, to encrypt video data in software. It is fast ...

Keywords: data security, multimedia com-munication, real-time video encryption, video compression

6 Security: Are parameterised biorthogonal wavelet filters suited (better) for selective encryption?

Andreas Uhl, Andreas Pommer
September 2004 **Proceedings of the 2004 workshop on Multimedia and security MM&Sec '04**
Publisher: ACM Press
Full text available: pdf(602.32 KB) Additional Information: full citation, abstract, references, citings, index terms

Selective encryption is used to encrypt parts of a bitstream, in our case images which are compressed by a wavelet based method. One approach is to keep the filter secret which is used for the transformation. Parameterised wavelet filters can be used to generate a large keyspace, however, in the case of orthogonal filters obtained by a variant of Pollen's factorisation it turns out that different parameters yield filters with very different quality and in particular worse quality as compared to ...

Keywords: biorthogonal wavelet filters, filter parameterisation, image compression,

image encryption, selective encryption

7 Hardware Engines for Bus Encryption: A Survey of Existing Techniques

R. Elbaz, L. Torres, G. Sassatelli, P. Guillemin, C. Anguille, M. Bardouillet, C. Buatois, J. B. Rigaud

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**

Publisher: IEEE Computer Society

Full text available: pdf(194.68 KB) Additional Information: full citation, abstract, index terms

The widening spectrum of applications and services provided by portable and embedded devices bring a new dimension of concerns in security. Most of those embedded systems (pay-TV, PDAs, mobile phones, etc...) make use of external memory. As a result, the main problem is that data and instructions are constantly exchanged between memory (RAM) and CPU in clear form on the bus. This memory may contain confidential data like commercial software or private contents, which either the end-user or the c ...

8 Coding and Encryption: On error preserving encryption algorithms for wireless video transmission

Ali Saman Saman Tosun, Wu-chi Feng

October 2001 **Proceedings of the ninth ACM international conference on Multimedia MULTIMEDIA '01**

Publisher: ACM Press

Full text available: pdf(157.93 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we describe error preserving encryption mechanisms for transmission of vido over wireless networks. One of the main problems with the secure transmission of data over wireless networks is that the bit errors that occur need to typically be sesolved *before* decryption can begin. For vido straming applications, this is unacceptable due to the general requirement that video be presented to the user in a continuous manner with low latency. In this paper, we describe a systematic ...

Keywords: video encryption, wireless video transmission

9 Optimizing the energy consumed by secure wireless sessions: wireless transport layer security case study

Ramesh Karri, Piyush Mishra

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available: pdf(151.69 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we identified the various sources of energy consumption during the setup, operation and tear down of a secure wireless session by considering the wireless transport layer security protocol. Our analysis showed that data transfers during a secure wireless transaction, number and size of messages exchanged during secure session establishment and cryptographic computations used for data authentication and privacy during secure data transactions in that order are the main sources of en ...

Keywords: WTLS, energy-efficient, mobile, secure session, security, wireless

10 Efficient frequency domain video scrambling for content access control

Wenjun Zeng, Shawmin Lei

October 1999 **Proceedings of the seventh ACM international conference on Multimedia (Part 1) MULTIMEDIA '99**
Publisher: ACM Press
Full text available: pdf(1.65 MB) Additional Information: full citation, abstract, references, index terms

Multimedia data security is very important for multimedia commerce on the Internet such as video-on-demand and real-time video multicast. Traditional cryptographic algorithms for data security are often not fast enough to process the vast amount of data generated by the multimedia applications to meet the real-time constraints. This paper presents a joint encryption and compression framework in which video data are scrambled efficiently in the frequency domain by employing selective bit scr ...

Keywords: compression, content access control, multimedia commerce, multimedia encryption, multimedia security, selective encryption, video scrambling

11 Low power scalable encryption for wireless systems
James Goodman, Anantha P. Chandrakasan
January 1998 **Wireless Networks**, Volume 4 Issue 1
Publisher: Kluwer Academic Publishers
Full text available: pdf(7.39 MB) Additional Information: full citation, abstract, references, citings, index terms

Secure transmission of multimedia information (e.g., voice, video, data, etc.) is critical in many wireless network applications. Wireless transmission imposes constraints not found in typical wired systems such as low power consumption, tolerance to high bit error rates, and scalability. A variety of low power techniques have been developed to reduce the power of several encryption algorithms. One key idea involves exploiting the variation in computation requirements to dynamically vary th ...

12 Encryption: Parameterized biorthogonal wavelet lifting for lightweight JPEG 2000 transparent encryption
Dominik Engel, Andreas Uhl
August 2005 **Proceedings of the 7th workshop on Multimedia and security MM&Sec '05**
Publisher: ACM Press
Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, index terms

Lightweight encryption offers a cogent alternative to full encryption of visual content in application settings with clients of low processing power, e.g. mobile applications, as it counterbalances security demands and computational demands. We present a lightweight transparent encryption scheme for JPEG 2000 that is based on and integrated into the wavelet lifting scheme. Keys are constructed from parameterized biorthogonal filters. The proposed method comes at extremely low computational cost ...

Keywords: JPEG 2000, lightweight encryption, parameterized biorthogonal wavelet lifting, transparent encryption

13 Data protection: Searchable symmetric encryption: improved definitions and efficient constructions
Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(682.40 KB) Additional Information: full citation, abstract, references, index terms

Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties:

1. Both solutions are more efficient than all previous constant-round schemes. In particular, the work performed by the server per r ...

Keywords: multi-user, searchable encryption, searchable symmetric encryption, security definitions

14 A secure multicast protocol with copyright protection

Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain
April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2
Publisher: ACM Press

Full text available: pdf(301.97 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

Keywords: copyright protection, key distribution, multicast security, watermark

15 Cryptography and data security

Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

16 High dictionary compression for proactive password checking

Francesco Bergadano, Bruno Crispo, Giancarlo Ruffo
November 1998 **ACM Transactions on Information and System Security (TISSEC)**, Volume 1 Issue 1
Publisher: ACM Press

Full text available: pdf(141.89 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The important problem of user password selection is addressed and a new proactive password-checking technique is presented. In a training phase, a decision tree is generated based on a given dictionary of weak passwords. Then, the decision tree is used

to determine whether a user password should be accepted. Experimental results described here show that the method leads to a very high dictionary compression (up to 1000 to 1) with low error rates (of the order of 1%). A prototype implementat ...

Keywords: access control, decision trees, password selection, proactive password checking

17 Digital signets: self-enforcing protection of digital information (preliminary version)

Cynthia Dwork, Jeffrey Lotspiech, Moni Naor

July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing STOC '96**

Publisher: ACM Press

Full text available: pdf(1.24 MB) Additional Information: full citation, references, citings, index terms

18 Research sessions: security and privacy: Order preserving encryption for numeric data

Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu

June 2004 **Proceedings of the 2004 ACM SIGMOD international conference on Management of data SIGMOD '04**

Publisher: ACM Press

Full text available: pdf(188.60 KB) Additional Information: full citation, abstract, references, citings

Encryption is a well established technology for protecting sensitive data. However, once encrypted, data can no longer be easily queried aside from exact matches. We present an order-preserving encryption scheme for numeric data that allows any comparison operation to be directly applied on encrypted data. Query results produced are sound (no false hits) and complete (no false drops). Our scheme handles updates gracefully and new values can be added without requiring changes in the encryption of ...

19 Power modeling and optimization for embedded systems: Analyzing the energy consumption of security protocols

Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha

August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design ISLPED '03**

Publisher: ACM Press

Full text available: pdf(271.69 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of wireless data applications and services. While several security mechanisms and protocols have been developed in the context of the wired Internet, many new challenges arise due to the unique characteristics of battery powered embedded systems. In this work, we focus on an important constraint of such devices -- battery life -- and examine how it is impacted by the use of security protocols.We present a comprehensive analysis of the energy requirements of a ...

Keywords: 3DES, AES, DES, DSA, Diffie-Hellman, ECC, RSA, SSL, cryptographic algorithms, embedded system, energy analysis, handheld, low-power, security, security protocols

20 Technical poster session 1: multimedia analysis, processing, and retrieval: Enhancing security of frequency domain video encryption

Zheng Liu, Xue Li, Zhaoyang Dong

October 2004 **Proceedings of the 12th annual ACM international conference on**

Multimedia MULTIMEDIA '04

Publisher: ACM Press

Full text available: pdf(1.13 MB) Additional Information: full citation, abstract, references, index terms

A potential security problem in frequency domain video encryption is that some trivial information such as the distribution of DCT coefficients may leak out secret. To illuminate this problem, we performed a successful attack on video using the distribution information of DCT coefficients. Then, according to the weak points discovered, a novel video encryption algorithm, working on run-length coded data, is proposed. It has amended identified security problems, while preserving high efficienc ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	("5512977").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/19 22:44
L2	5145	(extract$3 remov$3 tak$3 delet$3) near4 (portion part chunk fragment) with compressed	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:46
L3	405	(extract$3 remov$3 tak$3 delet$3) near4 (portion part chunk fragment) with compressed same image	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:47
L4	0	(extract$3 remov$3 tak$3 delet$3) near4 (portion part chunk fragment) with compressed same lz adj compression	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:47
L5	4	(encrypting with compressed adj (data video image) with (chang$3 remov$3 delet$3 replac$3 eliminat$3)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:53
L6	868	(key with (acquir$3 generat$3 creat$3 deriv$3 produc$3 with compressed) adj (information data image video)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:52
L7	38	(key with (acquir$3 generat$3 creat$3 deriv$3 produc$3) with compressed adj (information data image video)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:53
L8	4	(encrypting with compressed adj (information data video image) with (chang$3 remov$3 delet$3 replac$3 eliminat$3)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:53
L9	1362	((726/26) or (726/33)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/19 22:58

EAST Search History

L10	183	L9 and compression	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 22:58
S1	130	(380/269).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/18 22:34
S2	5	("5029107" | "5380993" | "5388158" | "5452356" | "5563946").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/17 23:06
S3	1	("5512977").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/17 23:06
S4	5	(("5,388,158") or ("6,014,444") or ("6,178,243") or ("6,434,561") or ("6,557,102")).PN.	US-PGPUB; USPAT	OR	OFF	2007/07/18 21:32
S5	1	("20040264698").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/18 21:32
S6	1287	(726/26).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/18 22:34
S7	1357	((726/26) or (726/33)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/19 22:58
S8	92	(726/33).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/18 22:35
S9	27	("5805700").URPN.	USPAT	OR	ON	2007/07/19 17:49
S10	8	("5606612").URPN.	USPAT	OR	ON	2007/07/19 18:28
S11	1	("20030026423").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/19 19:44
S12	252	(encrypt$3 same (delet$3 extract$3 remov$3) with compressed)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 19:57
S13	12230	(delet$3 extract$3 remov$3) near2 compressed	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 20:10
S14	173	(delet$3 extract$3 remov$3) near2 compressed with (encrypt hide prevent mask)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/19 20:10

EAST Search History

S16	1	("20030026423").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/19 20:14
S17	1	("7155012").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/19 22:22

EAST Search History

S18	297	("20010030959" | "20020026587" | "20020046406" | "20020047915" | "20020059425" | "20020083317" | "20020083438" | "20020097322" | "20020108035" | "20020129243" | "20020150239" | "20020170053" | "20020184506" | "20020194613" | "20020196939" | "20030002854" | "20030009669" | "20030021412" | "20030026423" | "20030046686" | "20030063615" | "20030072555" | "20030077071" | "20030081630" | "20030081776" | "20030084284" | "20030097662" | "20030112333" | "20030118243" | "20030123664" | "20030123849" | "20030126086" | "20030133570" | "20030140257" | "20030145329" | "20030152224" | "20030152226" | "20030156718" | "20030159139" | "20030159140" | "20030159152" | "20030174837" | "20030188154" | "20030193973" | "20030198223" | "20030204717" | "20030226149" | "20030228018" | "20040003008" | "20040010717" | "20040028227" | "20040047470" | "20040049688" | "20040049690" | "20040049691" | "20040049694" | "20040078575" | "20040081333" | "20040091109" | "20040123094" | "20040139337" | "20040165586" | "20040187161" | "20040193550" | "20050004875" | "20050071669" | "20050169473" | "20050192904" | "3852519" | "4381481" | "4381519" | "4419693" | "4521853" | "4634808" | "4700387" | "4703351" | "4703352" | "4710811" | "4712238" | "4722003" | "4739510" | "4772947" | "4785361" | "4788589" | "4815078" | "4845560" | "4887296" | "4890161" | "4924310" | "4944006" | "4953023" | "4989245" | "4995080" | "5018197" | "5023710" | "5091936" | "5122873" | "5138659" | "5142537" | "5144662" | "5144664" | "5159452").PN. OR ("5196931" | "5208816" | "5237424" | "5237610" | "5241381" | "5247575" | "5258835" | "5319707" | "5319712" | "5325432" | "5327502" | "5341425" | "5359694" | "5379072" | "5398078" | "5400401" | "5416651" | "5416847" | "5420866" | "5428403" | "5434716" | "5438369" | "5444491" | "5455862" | "5469216" | "5471501" | "5473692" | "5481554" | "5481627"	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/19 20:16

EAST Search History

S19	167	S18 and compress$3	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/19 20:16